Policies and Procedures
POLICY: Information Systems Activity Review
Policy #20
Effective Date: April 2, 2014

Purpose: Monitoring Information System events is an essential safeguard for the ILHIE infrastructure. ILHIE Authority audit logs permit the monitoring of Protected Health Information that is requested, used, or disclosure through the ILHIE and will be used for the purposes of monitoring the appropriateness of ILHIE access.

Only appropriately authenticated Authorized Users are granted access to the ILHIE. The ILHIE Authority can identify each Authorized User that has requested, used or disclosed an Individual's Protected Health Information through the ILHIE. Additional information about the request, use or disclosure of an Individual's Protected Health Information may be available from the Participant.

Policy:

1.0 Information Systems Activity Review. The ILHIE Authority and Participants shall each implement procedures to regularly review records of its respective Information System activity, such as audit logs, access reports, and Security Incident tracking and reporting, to identify potential inappropriate access and verify compliance with access controls.

1.1 The ILHIE Authority, or its authorized designee, shall perform regular audits of the acquisitions, access, uses or, disclosures of Protected Health Information through the ILHIE, and will conduct appropriate evaluations, including a risk assessment, when any major ILHIE Authority System or business changes are implemented.

1.2 The ILHIE Authority shall conduct penetration testing and compliance audits of the ILHIE Authority's Information System. The ILHIE Authority is authorized to conduct compliance audits of a Participant's System.

1.3 The ILHIE Authority and Participants will maintain an audit log for the period required by Applicable Law. The information will be housed in a retrievable storage medium.

1.4 Upon request, the ILHIE Authority will make its audit logs that pertain to a Participant available to such Participant.

2.0 Audit Protocol. The ILHIE Authority and Participants shall each generate audit logs in a standardized format such as ATNA to record respective System access and activity, and shall review the generated audit logs on a routine basis.

2.1 The ILHIE Authority shall implement Security Assertion Markup Language ("SAML") assertions as a component of the ILHIE audit log in accordance with the SAML Assertions and ILHIE Authority policy. Participant ability to

pass SAML-compliant user authorization information is a technical requirement for connecting to the ILHIE, effective June 30, 2014.

3.0 **Detecting Security Incidents.** The ILHIE Authority and Participants shall each develop protocols to detect and identify System Security Incidents within their respective systems, in accordance with these Policies and Procedures, the Data Sharing Agreement, and Applicable Law.

3.1 The ILHIE Authority will address Security Incidents which utilize ILHIE technology or infrastructure or which allow unauthorized access to ILHIE technology, ILHIE infrastructure or Protected Health Information through the ILHIE in a timely manner.

3.2 Upon request and to the extent available, the ILHIE Authority will reasonably assist Participants in the procurement of additional detail not included in the ILHIE's standard audit log information, and assist the Participant in the investigation of any Security Incident suffered by the Participant, including the development and implementation of an appropriate corrective action plan.

4.0 **Coordination.** The ILHIE Authority will coordinate any follow-up actions related to a Security Incident with the appropriate Participant(s) in accordance with the Data Sharing Agreement, these Policies and Procedures and Applicable Law.

5.0 **Compliance.** Participant shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with these Policies and Procedures.

5.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with and adherence to these Policies and Procedures.

Procedures

Participant Procedures

Participants will comply with or implement the following procedures.

1.0 Audit its Authorized Users' activities in order to assess potential risks and vulnerabilities with regard to Protected Health Information and use of the ILHIE.

2.0 Take appropriate corrective measures and document Security Incident findings in accordance with these Policies and Procedures, the Data Sharing Agreement and Applicable Law.

ILHIE Authority Procedures

The ILHIE Authority will comply with or implement the following procedures.

1.0 Audit its Authorized Users' activities in order to assess potential risks and vulnerabilities with regard to Protected Health Information and use of the ILHIE.

2.0 Take appropriate corrective measures and document Security Incident findings in accordance with these Policies and Procedures, the Data Sharing Agreement and Applicable Law.

3.0 Report a summary of the findings from ILHIE Authority System activity reviews to the ILHIE Authority Data Security and Privacy Committee as necessary, but at a minimum on an annual basis.

Associated Policies & Procedures
45 C.F.R § 164.308(a)(1)(ii)(D)
Accounting of Disclosures
Breach Notification and Mitigation
Data Sharing Agreement
Enforcement
SAML Assertions and ILHIE Policy
Sanctions
User Authentication
User Authorization

Definitions
Applicable Law
Audit Trail and Node Authentication
Audit Log
Authorized Users
Electronic Protected Health Information
Participant
Security Assertion Markup Language
Security Incident
System